6712-01

This document is scheduled to be published in the Federal Register on 01/23/2023 and available online at **federalregister.gov/d/2023-00824**, and on **govinfo.gov**

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 64

[WC Docket No. 22-21; FCC 22-102; FR 122866]

Data Breach Reporting Requirements

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) begins the process to update and strengthen its data breach rule to provide greater protections to the public. We propose to expand the Commission's definition of "breach" to include inadvertent disclosures of customer information and seek comment on adopting a harm-based trigger for breach notifications. We also propose to require carriers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable after discovery of a breach. We also propose to eliminate the mandatory waiting period before notifying customers and instead require carriers to notify customers of CPNI breaches without unreasonable delay after discovery of a breach unless requested by law enforcement. We also propose to make changes to our TRS data breach reporting rule consistent with those we propose to our CPNI breach reporting rule.

DATES: Comments are due on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, and reply comments are due on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. Written comments on the Paperwork Reduction Act proposed information collection requirements must be submitted by the public, Office of Management and Budget (OMB), and other interested parties on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].**

ADDRESSES: You may submit comments, identified by WC Docket No. 22-21, by any of the following methods:

- Federal Communications Commission's Web Site: https://apps.fcc.gov/ecfs/. Follow the instructions for submitting comments.
- People with Disabilities: Contact the FCC to request reasonable accommodations (accessible format documents, sign language interpreters, CART, etc.) by e-mail: FCC504@fcc.gov or phone: 202-418-0530 or TTY: 202-418-0432.

For detailed instructions for submitting comments and additional information on the rulemaking process, see the SUPPLEMENTARY INFORMATION section of this document. In addition to filing comments with the Secretary, a copy of any comments on the Paperwork Reduction Act proposed information collection requirements contained herein should be submitted to the Federal Communications Commission via email to PRA@fcc.gov and to Nicole On'gele, FCC, via email to Nicole.Ongele@fcc.gov.

FOR FURTHER INFORMATION CONTACT: Melissa Kirkel, Competition Policy Division, Wireline Competition Bureau, at (202) 418-7958, melissa.kirkel@fcc.gov. For additional information concerning the Paperwork Reduction Act information collection requirements contained in this document, send an email to PRA@fcc.gov or contact Nicole On'gele at (202) 418-2991.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Notice of Proposed Rulemaking in WC Docket No. 22-21, adopted on December 29, 2022 and released on January 6, 2023. The full text of this document is available at https://docs.fcc.gov/public/attachments/FCC-22-102A1.pdf. To request materials in accessible formats for people with disabilities (e.g. braille, large print, electronic files, audio format, etc.) or to request reasonable accommodations (e.g. accessible format documents, sign language interpreters, CART, etc.), send an email to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at (202) 418–0530.

Pursuant to Sections 1.415 and 1.419 of the Commission's rules, 47 CFR 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the

first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: https://apps.fcc.gov/ecfs/.
- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.
- Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.
- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701. U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street NE
Washington, DC 20554
- Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. See FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy, Public Notice, DA 20-304 (March 19, 2020). https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy.

The proceeding this document initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules. Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or

otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.*, .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

This document contains proposed information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. Public and agency comments are due **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].**

Comments should address: (a) whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information shall have practical utility; (b) the accuracy of the Commission's burden estimates; (c) ways to enhance the quality, utility, and clarity of the information collected; (d) ways to minimize the burden of the collection of information on the respondents, including the use of automated collection techniques or other forms of information technology; and (e) way to further reduce the

information collection burden on small business concerns with fewer than 25 employees. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C. 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

Synopsis

I. NOTICE OF PROPOSED RULEMAKING

1. To better protect telecommunications customers and ensure that our rules keep pace with today's challenges, we propose a number of updates to our rule addressing telecommunications carriers' breach notification duties. We seek to ensure that affected customers, the Commission, and other federal law enforcement agencies receive the information they need in a timely manner so they can mitigate and prevent harm due to the breach and take action to deter future breaches. To identify best practices and to minimize burdens, we look to other federal and state breach laws as potential models for our rules.

2. We propose to expand the Commission's definition of "breach" to include inadvertent disclosures of customer information and seek comment on adopting a harm-based trigger for breach notifications. We also propose to require carriers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable after discovery of a breach. We also propose to eliminate the mandatory waiting period before notifying customers and instead require carriers to notify customers of CPNI breaches without unreasonable delay after discovery of a breach unless requested by law enforcement. We also seek comment on whether we should adopt minimum requirements for the content of customer breach notices. We also evaluate and seek comment on the impact of the Congressional disapproval of the *2016 Privacy Order* on the Commission's legal authority to issue the rules proposed herein for telecommunications carriers. Finally, we propose to make changes to our TRS data breach reporting rule consistent with those we propose to our CPNI breach reporting rule.

A. Defining "Breach"

3. *Inadvertent Disclosures.* We propose to expand the Commission's definition of "breach" to include inadvertent access, use, or disclosures of customer information and seek comment on our proposal. Our current rule, adopted in response to the practice of pretexting, defines a "breach" as "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI." While the practice of pretexting necessarily involves an intent to gain access to customer information, the intervening years since the adoption of our existing rule have demonstrated that the inadvertent exposure of customer information can result in the loss and misuse of sensitive information by scammers and phishers, and trigger a need to inform the affected individuals so that they can take appropriate steps to protect themselves and their information. Further, whether or not a breach was intentional may not always be immediately apparent, which may lead to legal ambiguity and under-reporting. We also believe that it is important that the Commission and law enforcement be made aware of any accidental access, use, or disclosures so that we can (1) investigate and advise carriers on how best to avoid future breaches, and (2) stand ready to investigate if and when any of the affected information falls prey to malicious actors. We anticipate that requiring notification for accidental breaches will encourage telecommunications carriers to adopt stronger data security practices and will help us identify and confront systemic network vulnerabilities. Do commenters agree with the foregoing analysis? Are there other policy factors the Commission should consider in determining whether to require disclosure for unintentional breaches? What are the benefits and burdens associated with this proposal? We note that state data breach laws overwhelmingly do not include an intent limitation, and we seek comment on how state and other federal data breach laws should influence the policy we adopt.

4. We seek comment on the impact of requiring reporting of accidental breaches on the number of reported breaches. Do commenters foresee a significant increase in the number of reported breaches? If so, how would our proposal affect reporting costs for telecommunications

carriers and is that burden outweighed by the benefits to customers, who may need to take actions to protect their personal and financial information whether or not the breach was intentional? Would removing the intentionality limit potentially risk over-notification of data breaches to customers? What would the impacts of over-notification be? Would the potential benefits outweigh any potential harm? To help us assess the burden to both carriers and consumers from requiring reporting of accidental breaches, we invite commenters to provide estimates on the total number of breaches they have detected over the past few years, as well as the number of people affected by those breaches, and the severity of the compromised CPNI.

5. We propose to revise our definition to define a breach as any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed CPNI. We seek comment on this proposal and other possible definitions. Should we retain the intent limitation in certain contexts? If so, what contexts and why? With only a few exceptions, the vast majority of state statutes include a provision exempting from the definition of breach a good-faith acquisition of covered data by an employee or agent of the company where such information is not used improperly or further disclosed. Should we include such an exemption in our definition of "breach" or is such a provision unnecessary or otherwise inadvisable? Is our proposed rule sufficient to capture all instances in which persons, either purposefully or inadvertently, gain access to, use, or disclose CPNI? If not, how should we revise our proposed rule to ensure that it does? We also seek comment on whether we should expand the definition of a breach to include situations where a telecommunications carrier or a third party discovers conduct that could have reasonably led to exposure of customer CPNI, even if it has not yet determined if such exposure occurred.

6. *Harm-Based Notification Trigger.* We seek comment on whether to forego requiring notification to customers or law enforcement of a breach in those instances where a telecommunications carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. Our current rule requires no showing of harm, instead

requiring that notification be furnished in every instance where a breach of a carrier's customers' CPNI has occurred, where such breach is defined as any instance when "a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."

7. We seek comment on the benefits and drawbacks of adopting a "harm-based" notification trigger. How would it impact consumers? Would it benefit consumers by avoiding confusion and "notice fatigue" with respect to breaches that are unlikely to cause harm? Recognizing that it is not only distressing, but time consuming and expensive, to deal with the fallout of a data breach, we seek comment on whether a harm-based notification trigger could save consumers the time, effort, and financial difficulty of changing their passwords, purchasing fraud alerts or credit monitoring, and freezing their credit in the wake of a breach that is not reasonably likely to result in harm. Alternatively, does a harm-based notification trigger risk that consumers would be unaware of important information regarding their CPNI? We note that a harm-based trigger has a basis in data breach notification frameworks employed by states, which generally do not require covered entities to notify customers of breaches when a determination is made that the breach is unlikely to cause harm. How should state and other data breach laws influence our analysis?

8. We also seek comment on the potential impacts of adopting a harm-based trigger on telecommunications carriers. Would a harm-based trigger allow carriers to better focus their resources on data security and ameliorating the harms caused by data breaches? Or to the contrary, would a harm-based trigger require carriers to unnecessarily expend resources determining whether particular breaches are reasonably likely to cause harm instead of more efficiently providing notice?

9. If we adopt a harm-based trigger, how should telecommunications carriers and the Commission determine the likelihood of misuse or harm? Should we identify a standard or set of factors that telecommunications carriers must consider to evaluate whether no harm to customers

is reasonably likely? If so, what factors should carriers consider in making their evaluation? We preliminarily believe that no single factor on its own (*e.g.*, basic encryption) is sufficient to make a determination regarding harm to customers. Do commenters agree? Do carriers have sufficient expertise and experience to determine whether a breach is likely to result in harm? Should we establish a rebuttable presumption of consumer harm unless and until a carrier demonstrates that no harm to consumers is reasonably likely to occur as a result of a breach?

10. We seek comment on whether we should clarify the definition of "misuse" or "harm." For example, should we construe "harm" broadly to encompass not only financial, but also physical and emotional harm, including reputational damage, personal embarrassment, and loss of control over the exposure of intimate personal details? Should we require telecommunications carriers to consider whether other information about the customers that may be available combined with CPNI could result in harm when determining whether notification is required? Should any harm-based trigger apply even where the data breached is encrypted? What are the potential enforcement and compliance implications associated with this approach? Should breaches without such "harm" be reported to the Commission even if not reported to customers? Should we require the carrier to consult with federal law enforcement and/or the Commission prior to determining that there is no reasonable likelihood of harm or misuse? We seek comment on whether there are other triggers we should consider for which notice would be unnecessary, such as the number of affected consumers or the length of time exposure occurred. Are there other factors that we should consider before requiring breach notifications? Should we adopt a harm-based trigger only if we require notices of unintentional breaches, or should we evaluate the two issues independently? We also seek comment on the current notification practices in the industry. How do carriers currently make decisions regarding whether to notify customers and law enforcement of a breach?

11. We seek comment on whether any harm-based notification trigger should apply to both notifications to customers and notifications to law enforcement. While there are legitimate

reasons to consider eliminating notifications to customers in those instances where a breach is not reasonably likely to result in harm—including reducing confusion, stress, financial hardship, and notice fatigue—can the same be said of notifications to law enforcement? Are there compelling reasons for carriers to continue notifying law enforcement of data breaches even where such breaches are not reasonably likely to result in consumer harm? Do the benefits of notifying law enforcement of all breaches, regardless of whether the breach is likely to result in harm, outweigh the attendant costs to carriers of providing such notice?

12. We propose that if we adopt a harm-based trigger, where a carrier is unable to make a determination regarding harm or is uncertain whether harm is likely to occur, the obligation to notify would remain. We seek comment on this proposal.

13. We also recognize that telecommunications carriers possess proprietary information other than CPNI that customers have an interest in protecting from public exposure, such as Social Security Numbers and financial records. We seek comment on the Commission's authority to establish breach-reporting obligations for this type of information under Section 222, to the extent that this information is obtained by a telecommunications carrier in its activity as a common carrier. We also seek comment on the role of the Commission in protecting such information in light of the existing role of other agencies, including the FTC and Cybersecurity and Infrastructure Security Agency (CISA). If we were to require telecommunications carriers to report breaches of proprietary information other than CPNI under Section 222(a), how broadly or narrowly should we define that category of information? If we were to extend our data breach rule to cover such information, how could we minimize duplicative reporting obligations from the FTC and CISA?

B. Notifying the Commission and other Federal Law Enforcement of Data Breaches

14. *Commission Notification*. We propose to require telecommunications carriers to notify the Commission of breaches, in addition to the Secret Service and FBI, as soon as

practicable, and seek comment on our proposal. Our proposal is consistent with other federal sector-specific laws, which require prompt notification to the relevant subject-matter agency. For example, both HIPAA and the Health Breach Notification Rule require notice to the department of Health and Human Services (HHS) and the FTC respectively. We seek comment on the benefits and costs of requiring notification to the Commission in addition to notifying the Secret Service and the FBI, as our existing rules require.

15. As discussed above, the Commission adopted its existing data breach rule to address concerns regarding pretexting practices. The Commission found that notifying law enforcement of CPNI breaches is consistent with the goal of protecting CPNI because it enables law enforcement to investigate the breach, "which could result in legal action against the perpetrators, thus ensuring that they do not continue to breach CPNI." Moreover, the Commission anticipated that law enforcement investigations into how breaches occurred would enable law enforcement to advise the carrier and the Commission to take steps to prevent future breaches of that kind. However, as we have seen in the years since our data breach rule was initially adopted, not all breaches of customer data are the result of criminal pretexting, which was Commission's sole focus in 2007. Large-scale security breaches can also be the result of lax or inadequate data security practices and employee training. Thus, we tentatively conclude that notification of breaches will provide Commission staff important information about data security vulnerabilities that Commission staff can help address and remediate. We anticipate that breach notification to the Commission will also shed light on carriers' ongoing compliance with our rules. We seek comment on these tentative conclusions. How much of an incremental burden is associated with notifying the Commission of data breaches as compared to the existing data breach notification requirement for the Secret Service and FBI? Are there any other government entities to which we should require data breach reporting, such as the FTC? What would be the benefits and burdens of doing so?

16. *Method of Notification*. We propose that the Commission create and maintain a

centralized portal for reporting breaches to the Commission and other federal law enforcement agencies, and we seek comment on our proposal. Our current breach notification rule requires that telecommunications carriers notify the FBI and Secret Service "through a central reporting facility" to which the Commission maintains a link on its website. We believe that the creation and operation by the Commission of a centralized reporting facility for reporting of breaches to the Commission, Secret Service, and FBI will streamline the notification process and improve federal coordination. Do commenters agree? Are there alternative mechanisms for breach reporting to the Commission and other federal law enforcement that we should consider instead, such as leveraging the existing central reporting facility? Are there existing notification resources that we can leverage? For example, could we leverage the CISA Incident Reporting System to minimize burdens on carriers?

17. We seek comment on how we can minimize data breach reporting burdens for telecommunications carriers. The recently-passed Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) requires covered entities to notify CISA of cyber security incidents and establishes an interagency Cyber Incident Reporting Council intended to streamline interagency cyber incident reporting. When implemented, CIRCIA will require covered entities to report cybersecurity incidents to CISA, except where covered entities "by law, regulation, or contract" are already required to report "substantially similar information to another Federal agency within a substantially similar timeframe," in which case the other agency will report the incident to CISA. To the extent that a breach of CPNI is a result of a cyber incident, we seek comment on whether there are any modifications to our proposed rules that would minimize potential duplicate reporting of such breaches.

18. *Contents.* We seek comment on applying our existing requirements regarding the contents of the data breach notification to federal law enforcement agencies to breaches reported to the Commission. Generally, the central reporting facility requires carriers to report information relevant to the breach, including carrier contact information; a description of the

breach incident; the method of compromise; the date range of the incident, approximate number of customers affected; an estimate of financial loss to the carriers and customers, if any; types of data breached; and the addresses of affected customers. We believe that the information currently submitted through the FBI/Secret Service reporting facility is largely sufficient, and that generally the same information should be reported under the rule we propose here. Do commenters agree? Are there any additional or alternative categories of information that should be included in these disclosures? For example, should we require telecommunications carriers to report, at a minimum, the information required under CIRCIA with the aim of minimizing potentially duplicate reporting requirements? Should we curtail or streamline any of the existing content requirements? For example, should we eliminate the requirement that carriers report the addresses of affected individuals to law enforcement and the Commission, to minimize the personal information reported to the Commission and law enforcement?

19. *Timeframe.* We seek comment on the appropriate timeframe for notifying the Commission and other federal law enforcement of a breach. Our current rule requires telecommunications carriers to notify the Secret Service and the FBI of all breaches of CPNI no later than seven business days after reasonable determination of the breach. We propose to require carriers to notify the Commission of a reportable breach contemporaneously with notification to other law enforcement agencies as soon as practicable after discovery of a breach. We believe that requiring carriers to notify the Commission, Secret Service, and FBI at the same time will minimize burdens on carriers, eliminate confusion regarding obligations, and streamline the reporting process, allowing carriers to free up resources that can be used to address the breach and prevent further harm. We seek comment on our proposal. Is "as soon as practicable after discovery of a breach" an appropriate timeframe for notifying law enforcement after reasonable determination of a CPNI breach? Or, should we maintain the current "no later than seven business days" standard? Is there an alternative timeframe we should adopt for reporting CPNI breaches to the Commission and other federal law enforcement such as 24 hours

or 72 hours as has been proposed in other contexts, or should we consider adopting a graduated timeframe? We also seek comment on whether we should clarify when a carrier should be treated as having "reasonably determined" that a breach has occurred. Should a carrier be held to have "reasonably determined" a breach has occurred when it has information indicating that it is more likely than not that there was a breach? Should we publish guidance on what constitutes a reasonable determination? Should we adopt a more definite standard?

20. *Threshold Trigger.* We seek comment on whether it is appropriate to set a threshold for the number of customers affected to require a breach report to the Commission, Secret Service, and/or FBI. We observe that breaches affecting smaller numbers of customers may not necessitate the same law enforcement attention as larger breaches because they may be less likely to reflect coordinated attacks on CPNI. Under our current rule, telecommunications carriers must notify federal law enforcement of *all* reportable breaches, regardless of the number of customers affected. Setting a threshold for the number of customers affected for breach reporting to the Secret Service and FBI could reduce the administrative burdens on carriers and law enforcement agencies from excessive reporting, and is consistent with many state statutes requiring notice to state law enforcement authorities, which require law enforcement notification of large breaches.

21. At the same time, establishing a threshold may limit our and our federal partners' abilities to remediate, investigate, and deter smaller breaches. Further, as the Commission has previously found, notification of all breaches could allow the Commission and federal law enforcement to be "better positioned than individual carriers to develop expertise about the methods and motives associated with CPNI breaches." Is this still the case, given the development of data breach law and practices since 2007? Should we adopt a threshold for reporting to federal law enforcement? If so, should the threshold be the same for the Commission as for federal law enforcement? If not, how should the threshold differ? What would be an appropriate threshold for reporting? Most states that adopt a threshold for reporting

to law enforcement or government agencies require reporting at 250, 500, or 1000 individuals affected. What reporting threshold would meet the needs of law enforcement and provide adequate safeguards? What are the benefits and drawbacks of setting a threshold, particularly for small carriers? If we adopt a threshold trigger, should we require carriers to maintain a record of smaller breaches that fall below the threshold and report such small breaches to the Commission in a report at the end of the year? What are the benefits and drawbacks to such an approach? Rather than a numerical threshold, should we instead consider requiring carriers to report only intentional breaches to law enforcement, but to report all breaches, whether intentional or inadvertent, to the Commission?

C. Customer Notification

22. *Notifying Customers of Data Breaches without Unreasonable Delay.* We propose to require telecommunications carriers to notify customers of CPNI breaches without unreasonable delay after discovery of a breach and notification to law enforcement, unless law enforcement requests a delay. We seek comment on our proposal. Our existing data breach rule prohibits telecommunications carriers from notifying customers or disclosing the breach to the public until at least seven full business days after notification to the Secret Service and FBI. In cases where a carrier believes that there is an extraordinarily urgent need to notify affected customers in order to avoid immediate and irreparable harm, our rules permit carriers to notify affected customers after consultation with relevant investigating agencies. In adopting the existing rule, the Commission concluded that once customers have been notified, a breach may become public knowledge, "thereby impeding law enforcement's ability to investigate the breach, identify the perpetrators, and determine how the breach occurred." In short, the Commission found, "immediate customer notification may compromise all the benefits of requiring carriers to notify law enforcement of CPNI breaches," and therefore a short delay was warranted.

23. We tentatively conclude that this existing approach is out-of-step with current

approaches regarding the urgency of notifying victims about breaches of their personal information. We tentatively conclude that our proposal better serves the public interest than our current rule because it increases the speed at which customers may receive the important information contained in a notice, except in those specific circumstances when law enforcement officials specifically request otherwise. We seek comment on our tentative conclusion. What are the benefits and drawbacks to such an approach? Is there any reason to maintain our current absolute bar to customer notification for a set period? Does our proposal to eliminate the seven business-day waiting period before notifying customers appropriately balance legitimate law enforcement needs with the customers' need to take action to timely protect their information after a breach? We seek comment on whether a "without unreasonable delay" notification requirement would allow carriers enough time to determine the scope and impact of a breach. Would prompt customer notification compromise a carrier's ability to discover the source of the breach, mitigate the loss of data, and ensure further data is not compromised?

24. Our proposed requirement is consistent with many existing data breach notification laws that require expedited notice but refrain from requiring a specific timeframe. For example, the GLBA requires customer notification "as soon as possible" after a determination that customer information has been misused. California law requires notification "be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement." Similarly, many state data breach statutes impose an "expeditiously as practicable" or "without unreasonable delay" standard instead of a set time limit for reporting. In addition, FTC guidance on addressing data breaches explains that "if you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused." How should state and other federal law influence the approach we adopt?

25. We seek comment on whether requiring notice to customers "without unreasonable delay" after discovery of a breach provides sufficient guidance as to the required

timeframe to notify customers. Should we adopt a different approach, such as a fixed number of days for notification, and if so what should we adopt? If we were to adopt a "without unreasonable delay" standard, we seek comment on whether we should provide guidance on a specific time period that would be considered "reasonable" for notification. For example, HIPAA requires notification to individuals "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach." The Health Breach Notification Rule also requires notification to individuals "without unreasonable delay and in no case later than 60 days after the discovery of a breach of security." Most states that impose an outside limit on when consumers must be notified of a breach require notification to affected consumers no later than 30, 45, or 60 days after discovery of a breach. What are the benefits and drawbacks to setting a definite time limit on notification while requiring notification without unreasonable delay?

26. We also seek comment on whether the same notification deadline should be applied to all carriers. Are there unique concerns or compliance barriers for small carriers that make prompt response unfeasible, such as resource availability or reliance on third-party cybersecurity services for breach detection? Should we adopt different notification requirements for small carriers? If so, what threshold should we establish for small carriers? Should we consider establishing any other exceptions to this proposed requirement? We also seek comment on whether we should take into consideration the scope of the breach, e.g., how many customers are affected, the type of information breach, in determining the appropriate timeframe for customer breach reporting.

27. We seek comment on how best to coordinate the timing of customer notification and federal law enforcement notification. Our current rule, providing for consecutive rather than simultaneous notification of federal law enforcement and customers, was adopted at the request of federal law enforcement. Is such an approach still necessary? Are there circumstances where it would be acceptable for carriers to notify customers and law enforcement simultaneously in certain instances? Given that nearly all, if not all, state data breach statutes subject the timing of

customer notification to legitimate law enforcement needs, we seek comment on whether it is necessary to provide any further guidance to help coordinate the timing of notice to customers with notice to the Commission and other federal law enforcement.

28. In addition, consistent with our current rules implementing Section 222, our proposed rules would allow a federal agency to direct a carrier to delay customer notification for an initial period of up to 30 days if such notification would interfere with a criminal investigation or national security. In circumstances when a carrier reasonably decides to consult with law enforcement, a short delay pending such consultation would likely be reasonable for purposes of a "without unreasonable delay" standard for customer notification. We seek comment on this proposal. We observe that HIPAA, the GLBA, and the Health Breach Notification Rules allow for a delay of customer notification if law enforcement determines notification to customers would "impede a criminal investigation or cause damage to national security," but only if law enforcement officials request such a delay. Both HIPAA and the Health Breach Notification Rule allow notification delays of up to 30 days if requested by law enforcement. Similarly, GLBA allows that "customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for a delay." Likewise, most, if not all, states permit delays in notifying affected consumers for legitimate law enforcement needs. We tentatively conclude that our proposal strikes an appropriate balance between the needs of law enforcement to have time to investigate criminal activity and the needs of customers to be notified of data breaches. Do commenters agree? We also observe that these other regimes appear to allow non-federal law enforcement to request a delay, whereas the Commission's rule currently allows only federal agencies to so request. Should our rule also allow carriers to delay notification upon request of non-federal law enforcement?

29. *Contents of Customer Breach Notification*. We seek comment on whether we should require customer breach notifications to include specific minimum categories of

information. Our current rules specify when and to whom breach notifications must be made, but do not address the content of such notifications. In adopting the current breach notification rules, the Commission declined to specify the precise content of the notice that must be provided to customers in the event of a security breach of CPNI, "leav[ing] carriers the discretion to tailor the language and method of notification to the circumstances." Nearly 15 years later, we now seek comment on whether it is appropriate to require a minimum amount of information to ensure that such data breach notifications contain actionable information that is useful to the consumer. We seek comment on the benefits to customers and carriers of requiring carriers to include minimum categories of information in customer data breach notices. Will having minimum consistent fields of information assist consumers in understanding the circumstances and nature of the breach and streamline notice practices for carriers? What are the drawbacks to doing so? Are there any legal barriers to adopting a rule that prescribes the minimum categories of information in these breach notices?

30. To so identify possible categories of information to require, we look to numerous state data breach statutes as well as existing federal guidance regarding data breach notices. All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have laws requiring private or governmental entities to notify individuals of breaches involving their personal information. Of these, many impose minimum content requirements on the notifications that must be transmitted to affected individuals in the wake of a data breach, including: the name and contact information for the entity reporting the breach; the date, estimated date, or estimated date range of the breach; a description of the breach incident; a description of the personally identifiable information that was used, disclosed, or accessed, or reasonably believed to have been used, disclosed, or accessed; any actions the entity is taking to remedy the situation and/or protect affected individuals; a brief list of steps that affected consumers can take to protect themselves and their information, such as contacting credit bureaus to ask that fraud alerts or credit freezes be placed on their credit reports; and contact

information for the FTC and any federal agency that assists consumers with matters of identity theft. Similarly, both the HIPAA Breach Notification Rule and guidance issued by the Federal Deposit Insurance Corporation (FDIC) in response to the GLBA impose minimum content requirements on data breach notifications. In its Data Breach Response Guide, the FTC advises companies on specific information that should be included in their breach notices to individuals, including describing what the company knows about the breach (how it happened, what information was taken, how the thieves have used the information (if known), what actions the company has taken to remedy the situation, what actions the company is taking to protect individuals, how to reach the relevant contact in the organization); the steps individuals can take, given the type of information exposed, and provide relevant contact information; current information about how to recover from identity theft; information about the law enforcement agency working on the case, if the law enforcement agency agrees that would help; encouraging people who discover that their information has been misused to report it to the FTC; and describing how the company will contact consumers in the future to help victims avoid phishing scams.

31. We seek comment on adapting these models to telecommunications carriers and requiring carriers to include, at a minimum, the following information in security breach notices to customers: (1) the date of the breach; (2) a description of the customer information that was used, disclosed, or accessed; (3) information on how customers, including customers with disabilities, can contact the carrier to inquire about the breach; (4) information about how to contact the Commission, FTC, and any state regulatory agencies relevant to the customer and the service; (5) if the breach creates a risk of identity theft, information about national credit reporting agencies and the steps customers can take to guard against identity theft, including any credit monitoring, credit reporting, or credit freezes the carrier is offering to affected customers; and (6) what other steps customers should take to mitigate their risk based on the specific categories of information exposed in the breach. Are the identified categories the correct

information to be included in data breach notices? Should we consider requiring any additional or alternative categories of information that carriers must include in customer breach notices? For example, would it be helpful to include a statement of whether the notification was delayed due to reporting requirements to law enforcement or a law enforcement investigation, and if so, the length of the delay to help explain to customers the time lapse between discovery of the breach and customer notification? Should we require notifications to include a list of the law enforcement and government entities that have been notified of the breach? Should we require carriers to include a brief description of how the carrier will contact consumers in the future regarding the breach to help consumers avoid phishing scams related to breaches? What are best practices for providing consumers with actionable information in a breach notification? We seek comment on what minimum required information appropriately balances empowering consumers to take the necessary steps to protect themselves and their information in the wake of a data breach and appropriately limiting burdens on telecommunications carriers. We also seek comment on whether adopting or adapting a set of existing notification contents requirements will help to create a measure of consistency across breach notifications and will benefit both consumers and carriers, particularly smaller carriers, by streamlining the manner and content of their response in the event of a data breach.

32. *Method of Customer Breach Notification*. We observe that many state regulations specify the form that notifications to customers may take, whether by physical mail, email, or telephone. We seek comment on whether we should adopt a similar requirement and, if so, on what form notifications to consumers should take. Is there a method or methods of notification that would make the most sense or be most beneficial to consumers? What are the benefits and burdens of imposing such a requirement?

D. TRS Breach Reporting

33. In 2013, the Commission adopted CPNI rules applicable to all forms of Telecommunications Relay Services (TRS), as well as to point-to-point video calls handled over

the video relay services (VRS) network. The Commission found that "for TRS to be functionally equivalent to voice telephone services, consumers with disabilities who use TRS are entitled to have the same assurances of privacy as do consumers without disabilities for voice telephone services." The CPNI rules for TRS include a breach notification rule that is equivalent to § 64.2011 in terms of the substantive protection provided to TRS users. The texts of the two provisions are virtually identical, except for the substitution of the term "TRS provider" for "telecommunications carrier" in § 64.5111. The only substantive difference is that under the TRS rule, after a TRS provider notifies law enforcement of a breach, it "shall file a copy of the notification with the Disability Rights Office of the Consumer and Governmental Affairs Bureau at the same time as when the TRS provider notifies the customers."

34. To maintain functional equivalency for TRS users, we propose to amend § 64.5111 so that it continues to provide equivalent privacy protection for TRS users. The amendments we propose for § 64.5111 are thus essentially the same as those proposed for users of telecommunications and interconnected VoIP services. That is, we propose: (1) to expand the Commission's definition of "breach" to include inadvertent disclosures of customer information; (2) to require TRS providers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable after discovery of a breach; and (3) to eliminate the mandatory waiting period to notify customers, instead requiring TRS providers to notify customers of CPNI breaches without unreasonable delay after discovery of a breach unless law enforcement requests a delay. Further, we seek comment on the following additional issues, raised above regarding § 64.2011, as they relate to TRS providers: (1) whether to adopt a harm-based trigger for breach notifications; (2) whether we should adopt minimum requirements for the content of customer breach notices; and (3) whether our rules should address breaches of sensitive personal information.

35. We seek comment on each of these proposals and their costs and benefits. Should updated data breach requirements for TRS providers be identical to those we adopt for providers

of telecommunications and interconnected VoIP services, or are there circumstances unique to TRS providers that warrant differences in their obligations regarding data breaches? Are any additional notification requirements necessary to ensure TRS users receive functionally equivalent privacy protection? If we adopt the proposed requirement that service providers notify the Commission of breaches via a centralized portal, is there any need to retain the current requirement that TRS providers submit a copy of any breach notification to the Disability Rights Office of the Consumer and Governmental Affairs Bureau? Finally, would TRS providers incur costs or other compliance burdens under the proposed amendments that are disproportionately greater than those incurred by providers of telecommunications and interconnected VoIP services, and if so, would the extent of such costs or burdens justify the application of different breach notification requirements to TRS?

36. *Legal Authority.* Section 225 of the Act directs the Commission to ensure that TRS are available to enable communication in a manner that is functionally equivalent to voice telephone services. In 2013, the Commission found that applying the privacy protections of the Commission's CPNI regulations to TRS users advances the functional equivalency of TRS. The Commission concluded further that the specific mandate of Section 225 to establish "functional requirements, guidelines, and operations procedures for TRS" authorizes the Commission to make the privacy protections of the Commission's CPNI regulations applicable to TRS users. In addition, the Commission found that extending the CPNI regulations to TRS users is ancillary to its responsibilities under Section 222 of the Act to telecommunications service subscribers that place calls to or receive calls from TRS users, because TRS call records include call detail information concerning all calling and called parties. Finally, the Commission determined that applying CPNI requirements to point-to-point video services provided by VRS providers is ancillary to its responsibilities under Sections 222 and 225.

37. We tentatively conclude that, for the same reasons cited in the *2013 VRS Reform Order*, these sources of authority for establishing the current CPNI rules for TRS authorize the

Commission to amend those rules to ensure that TRS users receive privacy protections equivalent to those proposed for users of telecommunications and VoIP services. We seek comment on this tentative conclusion.

E. Legal Authority

38. *Section 222.* We believe that Section 222 provides authority to adopt the breach notification rules for which we seek comment in this *Notice of Proposed Rulemaking*. We also tentatively conclude that we have authority to apply the rules proposed in this *Notice of Proposed Rulemaking* to interconnected VoIP providers. We seek comment on these tentative conclusions.

39. Section 222 of the Act governs telecommunications carriers in their use, disclosure, and protection of proprietary information that they obtain in the course of providing telecommunications services. Section 222(a) imposes a duty on carriers to "protect the confidentiality of proprietary information of, and relating to" customers, fellow carriers, and equipment manufacturers. Section 222(c) imposes more specific requirements on carriers as to the protection and confidentiality of CPNI. We tentatively conclude that both subsections provide us authority to adopt rules requiring telecommunications carriers and interconnected VoIP providers to address breaches of CPNI.

40. The Commission has long required carriers to report data breaches as part of their duty to protect the confidentiality of customers' information. We believe that the proposed revisions to the Commission's data breach reporting rule reinforce carriers' duty to protect the confidentiality of their customers' information. Data breach reporting requirements also reinforce our other rules addressing the protection of CPNI. For example, data breach notifications can meaningfully inform customer decisions regarding whether to give, withhold, or retract their approval to use or disclose their information. Similarly, we believe that requiring carriers to notify the Commission in the event of a data breach will better enable the Commission to identify and confront systemic network vulnerabilities and help investigate and advise carriers

on how best to avoid future breaches, also helping carriers to fulfill their duty under Section 222(a) to protect the confidentiality of their customers' information. We seek comment on this analysis.

41. *Interconnected VoIP*. We believe that we have authority under Section 222 and our ancillary jurisdiction to apply the rules we propose today to interconnected VoIP providers. In 2007, the Commission exercised ancillary jurisdiction to extend its Part 64 CPNI rules to interconnected VoIP services. Since then, interconnected VoIP providers have operated under these rules. Interconnected VoIP services remain within the Commission's subject matter jurisdiction and we believe that the application of customer privacy requirements to these services is "reasonably ancillary to the effective performance" of our statutory responsibility under Section 222. As the Commission explained in 2007, "American consumers [can reasonably] expect that their telephone calls are private irrespective of whether the call is made using the service of a wireline carrier, a wireless carrier, or an interconnected VoIP provider." Now, as then, extending Section 222's protections to interconnected VoIP service customers is also "necessary to protect the privacy of wireline or wireless customers that place calls to or receive calls from interconnected VoIP providers." In addition, in 2008, Congress ratified the Commission's decision to apply Section 222's requirements to interconnected VoIP services by adding language to Section 222 that expressly covers "IP-enabled voice service," defined expressly to incorporate the Commission's definition of "interconnected VoIP service." The 2008 revisions to Section 222 would not make sense if the privacy-related duties of subsections (a) and (c) did not apply to interconnected VoIP providers. We seek comment on this analysis.

42. We seek comment on whether there are other bases of authority on which we can rely to adopt the rules we propose and seek comment on today.

F. Impact of the Congressional Disapproval of the *2016 Privacy Order*

43. As noted above, in 2016, the Commission acted to revise its breach notification rule as part of a larger proceeding addressing privacy requirements for broadband internet access

service providers (ISPs). The rules the Commission adopted in the *2016 Privacy Order* applied to telecommunications carriers and interconnected VoIP providers in addition to ISPs, which had been classified as providers of telecommunications services in 2015. In 2017, however, Congress nullified those 2016 revisions to the Commission's CPNI rules under the Congressional Review Act.

44. As a threshold matter, we seek comment on the effect of the Congressional disapproval of the *2016 Privacy Order* under the Congressional Review Act. While we seek comment on a range of proposals in this item, we clarify that, in light of the Congressional resolution of disapproval, we are not seeking comment on "reissu[ing] . . . in substantially the same form," or on issuing "a new rule that is substantially the same as," the rule disapproved by Congress. More generally, though, we seek comment here on the effect and scope of the Congressional disapproval of the *2016 Privacy Order* for purposes of adopting rules that apply to telecommunications carriers.

G. Digital Equity Considerations

45. The Commission, as part of its continuing effort to advance digital equity for all, including people of color and others who have been historically underserved, marginalized, and adversely affected by persistent poverty and inequality, invites comment on any equity-related considerations and benefits (if any) that may be associated with the proposals and issues discussed herein. Specifically, we seek comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility.

II. PROCEDURAL MATTERS

46. *Initial Regulatory Flexibility Analysis*. As required by the Regulatory Flexibility Act, the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities of the policies and rules addressed in this document. The IRFA is set forth in Appendix B. Written public comments are requested on the IRFA. Comments must be filed by the deadlines for comments on the Notice of Proposed

Rulemaking indicated on the first page of this document and must have a separate and distinct heading designating them as responses to the IRFA. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of this Notice of Proposed Rulemaking, including the IRFA, to the Chief Counsel for Advocacy of the SBA.

47. *People with Disabilities*. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice).

III. INITIAL REGULATORY FLEXIBILITY ANALYSIS

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), the Commission has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities by the policies and rules proposed in this Notice of Proposed Rulemaking. The Commission requests written public comments on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments provided on the first page of the Notice of Proposed Rulemaking. The Commission will send a copy of the Notice of Proposed Rulemaking, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA). In addition, the Notice of Proposed Rulemaking and IRFA (or summaries thereof) will be published in the Federal Register.

A. Need for, and Objectives of, the Proposed Rules

2. The Commission first adopted a rule in 2007 requiring telecommunications carriers and interconnected Voice over Internet Protocol (VoIP) providers to notify customers and federal law enforcement of breaches of customer proprietary network information (CPNI) in the carriers' possession. In the almost decade and a half since that time, data breaches nationwide have increased in both frequency and severity in all industries. In the telecommunications industry, the public has suffered an increasing number of security breaches of customer information in recent years. Federal and state data breach laws covering other areas

have evolved since 2007. Those developments combined with our specific experience suggest opportunities for improvement in our own breach notification rule. Today, we begin the process to update and strengthen our data breach rule to provide greater protections to the public.

3. The Commission adopted the data breach rule, like the rest of the privacy safeguards adopted in the *2007 CPNI Order*, to address the problem of "pretexting," the practice of pretending to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records. In the almost 15 years since, it has become clear that breaches of customer information in many contexts extend far beyond pretexting in general or the specific type of pretexting addressed at that time and are increasing in scale and evolving in methodology. The increasing severity and diversifying methods of security breaches involving customer information can have lasting detrimental impacts on customers whose information has been breached.

4. To better protect telecommunications customers and ensure that our rules keep pace with today's challenges, we propose a number of updates to our rule addressing telecommunications carriers' breach notification duties. We seek to ensure that affected customers, the Commission, and other federal law enforcement agencies receive the information they need in a timely manner so they can mitigate and prevent harm due to the breach and take action to deter future breaches. To identify best practices and to minimize burdens, we look to other federal and state breach laws as potential models for our rules.

5. In this document, we propose to expand the Commission's definition of "breach" to include inadvertent disclosures of customer information and seek comment on adopting a harm-based trigger for breach notifications. We also propose to require carriers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable after discovery of a breach. We also propose to eliminate the mandatory waiting period before notifying customers and instead require carriers to notify customers of CPNI breaches without unreasonable delay after discovery of a breach unless law enforcement requests a delay. We also

seek comment on whether we should adopt minimum requirements for the content of customer breach notices, and we seek comment on whether our rules should address breaches of other types of sensitive personal information beyond CPNI. Finally, we propose to make changes to our TRS data breach reporting rule consistent with those we propose to our CPNI breach reporting rule.

B. Legal Basis

6. The legal basis for any action that may be taken pursuant to this Notice of Proposed Rulemaking is contained in Sections 1, 4(i), 4(j), 201, 202, 222, 225, 303(r), and 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154, 201, 202, 222, 225, 303(r), 332.

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

7. The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules and by the rule revisions on which the Notice of Proposed Rulemaking seeks comment, if adopted. The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction." In addition, the term "small business" has the same meaning as the term "small-business concern" under the Small Business Act. A "small-business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.

8. *Small Businesses, Small Organizations, Small Governmental Jurisdictions*. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three broad groups of small entities that could be directly affected herein. First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business

Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees. These types of small businesses represent 99.9 percent of all businesses in the United States, which translates to 32.5 million businesses.

9. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field." The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations. Nationwide, for tax year 2018, there were approximately 571,709 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.

10. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand." U.S. Census Bureau data from the 2017 Census of Governments indicate that there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States. Of this number there were 36,931 general purpose governments (county, municipal and town or township) with populations of less than 50,000 and 12,040 special purpose governments - independent school districts with enrollment populations of less than 50,000. Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."

1. Wireline Carriers

11. *Wired Telecommunications Carriers*. The U.S. Census Bureau defines this industry as establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this

industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry. Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.

12. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 5,183 providers that reported they were engaged in the provision of fixed local services. Of these providers, the Commission estimates that 4,737 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

13. *Local Exchange Carriers (LECs)*. Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include both incumbent and competitive local exchange service providers. Wired Telecommunications Carriers is the closest industry with an SBA small business size standard. Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 5,183 providers that reported they were fixed local exchange

service providers. Of these providers, the Commission estimates that 4,737 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

14. *Incumbent LECs*. Neither the Commission nor the SBA has developed a small business size standard specifically for incumbent local exchange services. Wired Telecommunications Carriers is the closest industry with an SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 1,227 providers that reported they were incumbent local exchange service providers. Of these providers, the Commission estimates that 929 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, the Commission estimates that the majority of incumbent local exchange carriers can be considered small entities.

15. *Competitive Local Exchange Carriers (Competitive LECs).* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include several types of competitive local exchange service providers. Wired Telecommunications Carriers is the closest industry with a SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 3,956 providers that reported they were competitive local exchange service providers. Of these providers, the Commission estimates that 3,808 providers

have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

16. *Interexchange Carriers (IXCs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for Interexchange Carriers. Wired Telecommunications Carriers is the closest industry with a SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 151 providers that reported they were engaged in the provision of interexchange services. Of these providers, the Commission estimates that 131 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, the Commission estimates that the majority of providers in this industry can be considered small entities.

17. *Cable System Operators (Telecom Act Standard).* The Communications Act of 1934, as amended (the Act), also contains a size standard for small cable system operators, which is "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than one percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000." For purposes of the Telecom Act Standard, the Commission determined that a cable system operator that serves fewer than 677,000 subscribers, either directly or through affiliates, will meet the definition of a small cable operator based on the cable subscriber count established in a 2001 Public Notice. Based on industry data, only six cable system operators have more than 677,000 subscribers. Accordingly, the Commission estimates that the majority of cable system operators are small under this size standard. We note however, that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual

revenues exceed $250 million. Therefore, we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

18. *Other Toll Carriers.* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to other toll carriers. This category includes toll carriers that do not fall within the categories of interexchange carriers, operator service providers, prepaid calling card providers, satellite service carriers, or toll resellers. Wired Telecommunications Carriers is the closest industry with a SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 115 providers that reported they were engaged in the provision of other toll services. Of these providers, the Commission estimates that 113 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

2. Wireless Carriers

19. *Wireless Telecommunications Carriers (except Satellite)*. This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services. The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year. Of that number, 2,837 firms employed fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020,

there were 797 providers that reported they were engaged in the provision of wireless services. Of these providers, the Commission estimates that 715 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

20. *Satellite Telecommunications.* This category comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications." Satellite telecommunications service providers include satellite and earth station operators. The SBA small business size standard for this industry classifies a business with $38.5 million or less in annual receipts as small. U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year. Of this number, 242 firms had revenue of less than $25 million. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 71 providers that reported they were engaged in the provision of satellite telecommunications services. Of these providers, the Commission estimates that approximately 48 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, a little more than of these providers can be considered small entities.

3. Resellers

21. *Local Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Local Resellers. Telecommunications Resellers is the closest industry with a SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry. The

SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year. Of that number, 1,375 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 293 providers that reported they were engaged in the provision of local resale services. Of these providers, the Commission estimates that 289 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

22. *Toll Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Toll Resellers. Telecommunications Resellers is the closest industry with a SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry. The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year. Of that number, 1,375 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 518 providers that reported they were engaged in the provision of toll services. Of these providers, the Commission estimates that 495 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

23. *Prepaid Calling Card Providers.* Neither the Commission nor the SBA has developed a small business definition specifically for prepaid calling card providers.

Telecommunications Resellers is the closest industry with a SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry. The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year. Of that number, 1,375 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 58 providers that reported they were engaged in the provision of payphone services. Of these providers, the Commission estimates that 57 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

4. Other Entities

24. *All Other Telecommunications*. This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems. Providers of Internet services (e.g. dial-up ISPs) or voice over Internet protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry. The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small. U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated

for the entire year. Of those firms, 1,039 had revenue of less than $25 million. Based on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

25. In this document, we propose to expand the Commission's definition of "breach" to include inadvertent disclosures of customer information and seek comment on adopting a harm-based trigger for breach notifications. We also propose to require carriers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable after discovery of a breach. We also propose to eliminate the mandatory waiting period before notifying customers and instead require carriers to notify customers of CPNI breaches without unreasonable delay after discovery of a breach unless law enforcement requests a delay. We also seek comment on whether we should adopt minimum requirements for the content of customer breach notices, and we seek comment on whether our rules should address breaches of other types of sensitive personal information beyond CPNI. Finally, we propose to make changes to our TRS data breach reporting rule consistent with those we propose to our CPNI breach reporting rule.

26. Should the Commission decide to modify existing rules or adopt new rules to strengthen our data breach reporting rule, such action could potentially result in increased, reduced, or otherwise modified recordkeeping, reporting, or other compliance requirements for affected providers of service. We seek comment on the effect of any proposals on small entities. Entities, especially small businesses, are encouraged to quantify the costs and benefits of any reporting, recordkeeping, or compliance requirement that may be established in this proceeding.

E. Steps Taken to Minimize the Significant Economic Impact on Small Entities,

and Significant Alternatives Considered

27. The RFA requires an agency to describe any significant alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): (1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rules for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities.

28. The document seeks comment on the particular impacts that the proposed rules may have on small entities. Specifically, the document seeks comment on whether there are unique concerns or compliance barriers for small carriers that make notice to customers without unreasonable delay unfeasible; if there should be different notification requirements for small carriers; if streamlining notice requirements will benefit small providers; if a centralized reporting portal would reduce compliance barriers for small providers; and if a threshold trigger would benefit small providers.

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

29. None.

IV. ORDERING CLAUSES

30. Accordingly, IT IS ORDERED that, pursuant to Sections 1, 2, 4(i), 4(j), 201, 202, 222, 225, 303(b), 303(r), 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154(i), 154(j), 201, 202, 222, 225, 303(b), 303(r), 332, this Notice of Proposed Rulemaking IS ADOPTED.

31. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Notice of Proposed Rulemaking, including the Initial Regulatory Flexibility Analysis (IRFA), to

the Chief Counsel for Advocacy of the Small Business Administration.

List of Subjects in 47 CFR Part 64

Communications, Communications common carriers, Communications equipment, Individuals with disabilities, Reporting and recordkeeping requirements, Security measures, Telecommunications, Telephone

FEDERAL COMMUNICATIONS COMMISSION

Marlene Dortch,
Secretary.

For the reasons discussed in the preamble, the Federal Communications Commission proposes to amend 47 part 64 as follows:

PART 64 – MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

1. The authority citation for part 64 continues to read as follows:

Authority: 47 U.S.C. 151, 152, 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 255, 262, 276, 403(b)(2)(B), (c), 616, 617, 620, 1401-1473, unless otherwise noted; Pub. L. 115-141, Div. P, sec. 503, 132 Stat. 348, 1091.

Subpart U – Customer Proprietary Network Information

2. Amend § 64.2011 by revising paragraphs (a) through (e) to read as follows:

§ 64.2011 Notification of customer proprietary network information security breaches.

(a) A telecommunications carrier shall notify affected customers, the Federal Communications Commission (Commission), and other federal law enforcement of a breach of its customers' CPNI as provided in this section.

(b)(1) As soon as practicable after reasonable determination of a breach, a telecommunications carrier shall electronically notify the Commission, the United States Secret Service (USSS), and the Federal Bureau of Investigation (FBI) through a central reporting facility maintained by the Commission and made available on its website.

(2) If a law enforcement or national security agency notifies the carrier that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the carrier not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier when it appears that public disclosure or notice to affected customers

will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security.

(c) Customer Notification. A telecommunications carrier shall notify affected customers of covered breaches of CPNI without unreasonable delay after discovery of the breach after notification to the Commission and law enforcement as described in paragraph (b) of this section.

(d) Recordkeeping. All carriers shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the Federal Communications Commission, USSS, and the FBI pursuant to paragraph (b) of this section, and notifications made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Carriers shall retain the record for a minimum of 2 years.

(e) Definitions. As used in this section, a "breach" has occurred when a person, without authorization or exceeding authorization, has gained access to, used, or disclosed CPNI.

* * * * *

3. Amend § 64.5111 by revising paragraphs (a) through (e) to read as follows:

§ 64.5111 Notification of customer proprietary network information security breaches.

(a) A TRS provider shall notify affected customers, the Federal Communications Commission (Commission), and other federal law enforcement of a breach of its customers' CPNI as provided in this section.

(b)(1) As soon as practicable after reasonable determination of a breach, a TRS provider shall electronically notify the Commission, the United States Secret Service (USSS), and the

Federal Bureau of Investigation (FBI) through a central reporting facility maintained by the Commission and made available on its website.

(2) If a law enforcement or national security agency notifies the TRS provider that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the TRS provider not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the TRS provider when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the TRS provider, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by TRS provider .

(c) Customer Notification. A TRS provider shall notify affected customers of covered breaches of CPNI without unreasonable delay after discovery of the breach after notification to the Commission and law enforcement as described in paragraph (b) of this section.

(d) Recordkeeping. All TRS provider shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the Federal Communications Commission, USSS, and the FBI pursuant to paragraph (b) of this section, and notifications made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. TRS providers shall retain the record for a minimum of 2 years.

(e) Definitions. As used in this section, a “breach” has occurred when a person, without authorization or exceeding authorization, has gained access to, used, or disclosed CPNI.

* * * * *

[FR Doc. 2023-00824 Filed: 1/20/2023 8:45 am; Publication Date: 1/23/2023]